BUNDESREPUBLIK DEUTSCHLAND

OIPE
MAY 17 2000
PATENT & TRADEMARK OFFICE
JC90

Bescheinigung

Die Giesecke & Devrient GmbH in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zum Austauschen von mindestens einem geheimen Anfangswert zwischen einer Bearbeitungsstation und einer Chipkarte"

am 25. Januar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 06 K 19/06 der Internationalen Patentklassifikation erhalten.

München, den 2. Februar 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Wehner

Aktenzeichen: 199 02 722.6

CERTIFIED COPY OF PRIORITY DOCUMENT

A 9161
06.90
11/98

Verfahren zum Austauschen von mindestens einem geheimen Anfangswert zwischen einer Bearbeitungsstation und einer Chipkarte

Die Erfindung betrifft ein Verfahren zum Austauschen von mindestens einem geheimen Anfangswert zwischen einer Bearbeitungsstation und einer Chipkarte, bei einem Initialisierungsschritt für die Chipkarte.

Derartige Verfahren sind bereits seit längerem bekannt und dienen bei der Herstellung von Chipkarten, die heute in vielen Bereichen, z.B. in Zugangskontrollsystemen oder als Zahlungsmittel verwendet werden, der sicheren Inbetriebnahme der Chipkarten. Die Chipkarte umfaßt üblicherweise einen integrierten Schaltkreis sowie Kopplungselemente, die leitend mit dem integrierten Schaltkreis verbunden sind und der Kommunikation mit externen Geräten, beispielsweise einer Bearbeitungsstation, dienen. Die Kopplungselemente sind entweder in Form von Kontaktflächen zur berührenden Kontaktabnahme oder auch als Spulen zur nicht berührenden Kontaktabnahme ausgebildet.

Bei den herkömmlichen Verfahren wird als letzter Schritt in der Herstellung der Chipkarte eine Initialisierung und Personalisierung der Chipkarte vorgenommen. Dabei werden die programmtechnischen Voraussetzungen geschaffen, alle Daten in den Speicherbereich des integrierten Schaltkreises zu laden, die für den späteren Betrieb der Chipkarte nötig sind. Bei der Initialisierung werden dazu alle global nötigen Daten übertragen und die nötigen Dateistrukturen angelegt. Bei der Personalisierung werden die individuellen Daten von der Bearbeitungsstation zur Chipkarte übertragen und in entsprechenden Speicherbereichen abgespeichert. Die zur Personalisierung benötigten Daten können beispielsweise Name, Anschrift und ein geheimer Schlüssel sein.

Um zu gewährleisten, daß die Personalisierungsdaten, insbesondere beispielsweise ein geheimer Schlüssel, bei der Personalisierung nicht abgehört werden können, um späteren Mißbrauch zu vermeiden, wird nach dem bekannten Verfahren üblicherweise die Initialisierung und Personalisierung in getrennten Prozeßschritten und auch teilweise in getrennten Räumen mit unterschiedlichem Personal durchgeführt. Während der Initialisierung wird dazu beispielsweise eine auf der Chipkarte gespeicherte Seriennummer an die Bearbeitungsstation übertragen. Zur Übertragung weist die Bearbeitungsstation ein Terminal auf. Außerdem ist in der Bearbeitungsstation üblicherweise ein Sicherheitsmodul vorhanden, an welches das Terminal die Nummer der Chipkarte weiterleitet. Im Sicherheitsmodul wird mit der Nummer der Chipkarte ein Schlüssel erzeugt, der an die Chipkarte mittels des Terminals übertragen wird.

Im nachfolgenden Personalisierungsschritt werden Daten aus einer Datenbank, die die zur Personalisierung nötigen Daten enthält, zur Chipkarte übertragen und in den entsprechenden Speicherbereichen der Chipkarte abgespeichert. Die Personalisierungsdaten der Personalisierungsdatenbank liegen üblicherweise verschlüsselt vor. Um einen Mißbrauch zu vermeiden, ist der Schlüssel zur Entschlüsselung der Personalisierungsdaten dem Hersteller der Chipkarte normalerweise nicht bekannt. Dieser Schlüssel ist nur der Institution bekannt, die die Personalisierungsdaten zur Verfügung stellt, beispielsweise einer Bank, die die als Zahlungsmittel verwendete Chipkarte ausstellt. Zur weiteren Verarbeitung der verschlüsselten Personalisierungsdaten werden diese ins Sicherheitsmodul der Bearbeitungsstation geladen. Das Sicherheitsmodul bietet eine separate Einheit, die besonders gegen Manipulationsversuche geschützt ist. Im Sicherheitsmodul ist der zur Entschlüsselung der Personalisierungsdaten benötigte Schlüssel enthalten. Mittels dieses Schlüssels werden die Personalisierungsdaten im Sicherheitsmo-

dul entschlüsselt und anschließend mit dem bei der Initialisierung erzeugten Schlüssel, der zuvor vom Sicherheitsmodul aus in die Chipkarte geladen wurde, erneut verschlüsselt. Die so verschlüsselten Daten werden vom Sicherheitsmodul aus über das Terminal an die Chipkarte übertragen. Anschließend werden in der Chipkarte die verschlüsselten Daten mit dem bekannten Schlüssel entschlüsselt und in den entsprechenden Speicherbereichen des integrierten Schaltkreises der Chipkarte abgespeichert.

Das bekannte Verfahren weist somit den Nachteil auf, daß zumindest zu einem Zeitpunkt, nämlich bei der Initialisierung der Chipkarte, ein zur Datenübertragung zwischen einer Bearbeitungsstation und einer Chipkarte benötigter geheimer Schlüssel einmalig im Klartext übertragen werden muß. Falls dieser Schlüssel abgehört wird, können alle im später nachfolgenden Personalisierungsschritt übertragenen Daten und geheimen Schlüssel entschlüsselt werden. Falls es sich um einen kartenindividuellen Schlüssel handelt, wäre zumindest die Sicherheit dieser einen Karte gebrochen.

Aufgabe der vorliegenden Erfindung ist es deshalb, ein Verfahren zum Austauschen von mindestens einem geheimen Anfangswert zwischen einer Bearbeitungsstation und einer Chipkarte, bei der Initialisierung der Chipkarte, anzugeben, das gegenüber dem Stand der Technik eine größere Sicherheit aufweist und einfacher eingesetzt werden kann.

Die Aufgabe wird durch die Merkmale des Anspruchs 1 gelöst.

Die Erfindung geht dabei von der Überlegung aus, daß zu keinem Zeitpunkt zwischen der Bearbeitungsstation und der Chipkarte sensible Daten im Klartext übertragen werden. Dies wird dadurch erreicht, daß sowohl in der Bearbeitungsstation als auch in der Chipkarte Werte erzeugt werden, die nur

zum Teil jeweils an die Chipkarte bzw. die Bearbeitungsstation übertragen werden. Aus den erzeugten und den übertragenen Werten werden dann sowohl in der Chipkarte als auch in der Bearbeitungsstation die geheimen Daten ermittelt.

Der besondere Vorteil der Erfindung liegt darin, daß zu keinem Zeitpunkt während der Initialisierung bzw. eines sich daran anschließenden Personalisierungsschritts geheime Daten im Klartext zwischen Bearbeitungsstation und Chipkarte übertragen werden müssen. Dadurch wird zum einen die Sicherheit des Initialisierungs- und Personalisierungsschritts erhöht, zum anderen vereinfacht sich die Initialisierung und Personalisierung, weil diese nicht mehr in getrennten Schritten durchgeführt werden müssen. Durch die dadurch erfolgende Reduzierung des nötigen Sicherheitsaufwands ergibt sich auch eine Reduzierung des Kostenaufwands bei der Chipkartenherstellung.

Weitere Vorteile der vorliegenden Erfindung ergeben sich aus den abhängigen Ansprüchen sowie der nachfolgenden Beschreibung anhand einer Figur.

Die einzige Figur zeigt eine Bearbeitungsstation und eine Chipkarte bei der Initialisierung bzw. Personalisierung der Chipkarte.

In der Figur ist eine Bearbeitungsstation S, eine Chipkarte CC und eine Datenbank DB dargestellt. Die Bearbeitungsstation S enthält ein Terminal T das den Datenaustausch mit der Chipkarte CC herstellt sowie ein Sicherheitsmodul HSM, das zur Verarbeitung geheimer Daten dient. Diese geheimen Daten können beispielsweise von der Datenbank DB stammen. Außerdem ist in der Figur ein Initialisierungsschritt IS und ein Personalisierungsschritt PS dargestellt.

Wird eine neue Chipkarte CC zur Initialisierung in Verbindung mit dem Terminal T der Bearbeitungsstation S gebracht, kann zunächst die Echtheit der Chipkarte CC überprüft werden. Dies ist nötig, um auszuschließen, daß unberechtigte Chipkarten initialisiert werden und auf diese Weise unberechtigt an geheime Daten gelangen. Zur Überprüfung der Echtheit der Chipkarte CC kann beispielsweise überprüft werden, ob der auf der Chipkarte vorhandene integrierte Schaltkreis einem bestimmten Hersteller zuzuordnen ist. Zusätzlich kann außerdem eine Seriennummer, die bei der Herstellung des integrierten Schaltkreises erzeugt wurde, überprüft werden. Dazu wird die Seriennummer des auf der Chipkarte CC befindlichen integrierten Schaltkreises über das Terminal T ausgelesen. Die so ermittelte Seriennummer des integrierten Schaltkreises der Chipkarte CC wird anschließend im Sicherheitsmodul HSM auf Zulässigkeit überprüft. Dazu wird eine in der Datenbank DB abgelegte Liste von Seriennummern überprüft.

Nach erfolgter Echtheitsüberprüfung werden im Sicherheitsmodul HSM Werte erzeugt, die der Bestimmung eines geheimen Anfangswerts dienen, wobei der geheime Anfangswert im Sicherheitsmodul HSM und in der Chipkarte CC gleich sind, ohne daß der geheime Anfangswert im Klartext vom Sicherheitsmodul HSM über das Terminal T zur Chipkarte CC übertragen wird. Teile der Werte, die im Sicherheitsmodul HSM erzeugt wurden, werden über das Terminal T an die Chipkarte CC übertragen. In der Chipkarte CC werden weitere Werte zur Bestimmung des geheimen Anfangswerts erzeugt, von denen wiederum Teile an die Bearbeitungsstation S über das Terminal T übertragen werden. Anschließend wird der geheime Anfangswert in der Bearbeitungsstation, d.h. im Sicherheitsmodul HSM, aus den Werten, die im Sicherheitsmodul HSM erzeugt wurden und den von der Chipkarte übertragenen Werten bestimmt. In der Chipkarte CC erfolgt die

Bestimmung des geheimen Anfangswerts mittels der in der Chipkarte erzeugten Werte und den von der Bearbeitungsstation übertragenen Werten.

Der geheime Anfangswert kann beispielsweise ein Startwert für die Erzeugung von Zufallszahlen sein. Außerdem kann der geheime Anfangswert auch als geheimer Schlüssel für die Verschlüsselung und Entschlüsselung von Daten verwendet werden.

Wird der geheime Anfangswert als Schlüssel verwendet, können beispielsweise in einem nachfolgenden Bearbeitungsschritt Personalisierungsdaten, die unter anderem weitere geheime Schlüssel enthalten, an die Chipkarte CC übertragen werden.

Der geheime Anfangswert kann aus den im Sicherheitsmodul HSM und in der Chipkarte CC erzeugten Werten beispielsweise mittels Algorithmen oder Funktionen erzeugt werden. Besonders vorteilhaft ist es, wenn sowohl im Sicherheitsmodul HSM als auch in der Chipkarte CC zur Erzeugung des geheimen Anfangswertes die gleiche Funktion verwendet wird. Dazu ist in der Figur für den Initialisierungsschritt IS eine Funktion vorgesehen, die eine erste Variable oder einen ersten Wert mit einem zweiten Wert potenziert und ein Modulorest zu einem dritten Wert gebildet wird. Im Sicherheitsmodul HSM werden die Werte g, n und x erzeugt. Der Wert n ist eine große Primzahl, der Wert g eine primitive Zahl, d.h., alle Zahlen 1....n-1 können in der Form $g^i \bmod n$ dargestellt werden. Zur Erhöhung der Sicherheit sollte sichergestellt werden, daß der Wert (n-1)/2 ebenfalls eine Primzahl ist. Der außerdem im Sicherheitsmodul HSM erzeugte Wert x ist eine Zufallszahl, für die gilt $x < n$. Mittels der Funktion

$$(1) \qquad X = g^x \bmod n$$

werden die Werte g n und X verarbeitet. Anschließend werden die Werte g, n und X über das Terminal T an die Chipkarte CC übertragen. Der Wert x wird im Sicherheitsmodul geheimgehalten. In der Chipkarte wird mittels einer weiteren Funktion

$$(2) \qquad Y = g^y \bmod n$$

ein Wert Y erzeugt. Dazu werden die von der Bearbeitungsstation übertragenen Werte g und n sowie ein in der Chipkarte erzeugter Wert y verwendet. Für den Wert y gilt $y < n$. Der Wert y ist eine Zufallszahl, die insbesondere in Abhängigkeit einer individuellen Kennung der Chipkarte CC, z.B. einer Seriennummer, erzeugt wird. Der Wert y wird in der Chipkarte CC geheimgehalten, wohingegen der Wert Y an die Bearbeitungsstation S übertragen wird. In der Bearbeitungsstation S wird im Sicherheitsmodul HSM mittels einer Funktion

$$(3) \qquad K = Y^x \bmod n$$

der geheime Anfangswert, der als Schlüssel verwendet wird, erzeugt. In der Chipkarte CC wird der gleiche geheime Anfangswert K erzeugt

$$(4) \qquad K = X^y \bmod n.$$

Die Gleichheit des geheimen Anfangswerts K in Chipkarte CC und Sicherheitsmodul HSM ist gewährleistet, da wegen des Austauschs der Werte zwischen Chipkarte CC und Sicherheitsmodul HSM für K gilt:

$$(5) \qquad K = g^{xy} \bmod n.$$

Mittels des nunmehr sowohl im Sicherheitsmodul HSM als auch in der Chipkarte CC vorhandenen geheimen Schlüssels K kann in einem nachfolgenden Personalisierungsschritt PS die sichere Übertragung geheimer Personalisierungsdaten vorgenommen werden. Dazu werden aus der Datenbank DB Personalisierungsdaten PD_{KM}, die mit einem Hauptschlüssel KM verschlüsselt sind, an das Sicherheitsmodul HSM übertragen. Der Hauptschlüssel KM ist im Sicherheitsmodul HSM vorhanden und wird zur Dekodierung der Personalisierungsdaten PD_{KM} verwendet. Die nunmehr im Klartext vorliegenden Personalisierungsdaten PD werden in einem weiteren Schritt wieder verschlüsselt. Dazu wird der geheime Schlüssel K verwendet. Die so erzeugten verschlüsselten Personalisierungsdaten PD_K werden über das Terminal T an die Chipkarte CC übertragen, wo sie mit dem ebenfalls vorhandenen geheimen Schlüssel K dekodiert werden.

Nach Beendigung des Personalisierungsschritts PS kann der geheime Schlüssel K sowohl in der Chipkarte als auch im Sicherheitsmodul HSM gelöscht werden, da für die weitere Kommunikation zwischen Bearbeitungsstation S und Chipkarte CC beispielsweise die in den Personalisierungsdaten PD enthaltenen geheimen Schlüssel verwendet werden können.

Initialisierungs- und Personalisierungsschritte der oben beschriebenen Art können nicht nur bei der Herstellung von Chipkarten eingesetzt werden, wie eingangs erwähnt, sondern auch der späteren Erweiterung von Chipkarten dienen. Beispielsweise um eine Chipkarte nachträglich um weitere Anwendungen zu erweitern. Eine Chipkarte die

bisher nur als Kreditkarte konfiguriert war, kann z.B. um eine Zugangskontrollanwendung erweitert werden.

Patentansprüche

1. Verfahren zum Austauschen von mindestens einem geheimen Anfangswert zwischen einer Bearbeitungsstation und einer Chipkarte, bei einem Initialisierungsschritt für die Chipkarte, wobei
   - in der Bearbeitungsstation erste Werte zur Bestimmung des geheimen Anfangswerts erzeugt werden,
   - Teile der ersten Werte an die Chipkarte übertragen werden,
   - in der Chipkarte zweite Werte zur Bestimmung des geheimen Anfangswerts erzeugt werden,
   - Teile der zweiten Werte an die Bearbeitungsstation übertragen werden,
   - der geheime Anfangswert in der Bearbeitungsstation aus zumindest Teilen der ersten Werte und den übertragenen Teilen der zweiten Werte bestimmt wird, und
   - der geheime Anfangswert in der Chipkarte aus zumindest Teilen der zweiten Werte und den übertragenen Teilen der ersten Werte bestimmt wird.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß mindestens ein Teil der in der Chipkarte erzeugten zweiten Werte in Abhängigkeit von einer in der Chipkarte vorhandenen individuellen Kennung, insbesondere einer Seriennummer, erzeugt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, daß
   - die in der Bearbeitungsstation erzeugten ersten Werte einer ersten Funktion unterworfen werden,
   - das Ergebnis der ersten Funktion zusätzlich zum Teil der erzeugten ersten Werte an die Chipkarte übertragen wird,

- mindestens ein Teil der in der Chipkarte erzeugten zweiten Werte mit dem übertragenen Teil der ersten Werte einer zweiten Funktion unterworfen wird,
- das Ergebnis der zweiten Funktion an die Bearbeitungsstation übertragen wird,
- der geheime Anfangswert in der Bearbeitungsstation mittels einer dritten Funktion aus dem übertragenen Ergebnis der zweiten Funktion und einem Teil der ersten Werte, insbesondere dem nicht zur Chipkarte übertragenen ersten Teil der Werte, erzeugt wird, und
- der geheime Anfangswert in der Chipkarte mittels einer vierten Funktion aus dem übertragenen Ergebnis der ersten Funktion, dem übertragenen Teil der ersten Werte und mindestens einem Teil der zweiten Werte, insbesondere dem nicht zur Bearbeitungsstation übertragenen Teil der zweiten Werte, erzeugt wird.

4. Verfahren nach Anspruch 3, dadurch **gekennzeichnet**, daß erste, zweite, dritte und vierte Funktion gleich sind.

5. Verfahren nach Anspruch 4, dadurch **gekennzeichnet**, daß als Funktion eine erste Variable mit einer zweiten Variablen potenziert wird und ein Modulorest zu einer dritten Variablen gebildet wird, wobei die Variablen den ersten und zweiten Werten sowie dem ersten und zweiten Ergebnis entsprechen.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß der geheime Anfangswert ein Startwert für die Erzeugung von Zufallszahlen ist.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Austauschen von mindestens einem geheimen Anfangswert zwischen einer Bearbeitungsstation und einer Chipkarte, bei einem Initialisierungsschritt für die Chipkarte.

Bei bekannten Verfahren wird bei der Initialisierung der Chipkarten ein Anfangswert, z.B. ein Schlüssel, von einer Bearbeitungsstation zur Chipkarte übertragen und in dieser abgespeichert. Da dieser Schlüssel im Klartext übertragen wird, entstehen Sicherheitsprobleme.

Bei der vorliegenden Erfindung werden die geschilderten Sicherheitsprobleme dadurch gelöst, daß zwischen Bearbeitungsstation und Chipkarte nur Teile des Schlüssels ausgetauscht werden und der Schlüssel in der Chipkarte und der Bearbeitungsstation aus den Teilen erzeugt wird.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß der geheime Anfangswert ein Schlüssel für die Verschlüsselung und Entschlüsselung von Daten ist.

8. Verfahren nach Anspruch 7, dadurch **gekennzeichnet**, daß der in Bearbeitungsstation und Chipkarte erzeugte Schlüssel in einem Personalisierungsschritt zur Ver- und Entschlüsselung von Personalisierungsdaten, insbesondere weiteren geheimen Schlüsseln, verwendet wird, die von der Bearbeitungsstation zur Chipkarte übertragen werden.

9. Verfahren nach Anspruch 8, dadurch **gekennzeichnet**, daß der in der Bearbeitungsstation und der Chipkarte erzeugte Schlüssel nach dem Personalisierungsschritt in der Bearbeitungsstation und der Chipkarte gelöscht wird.

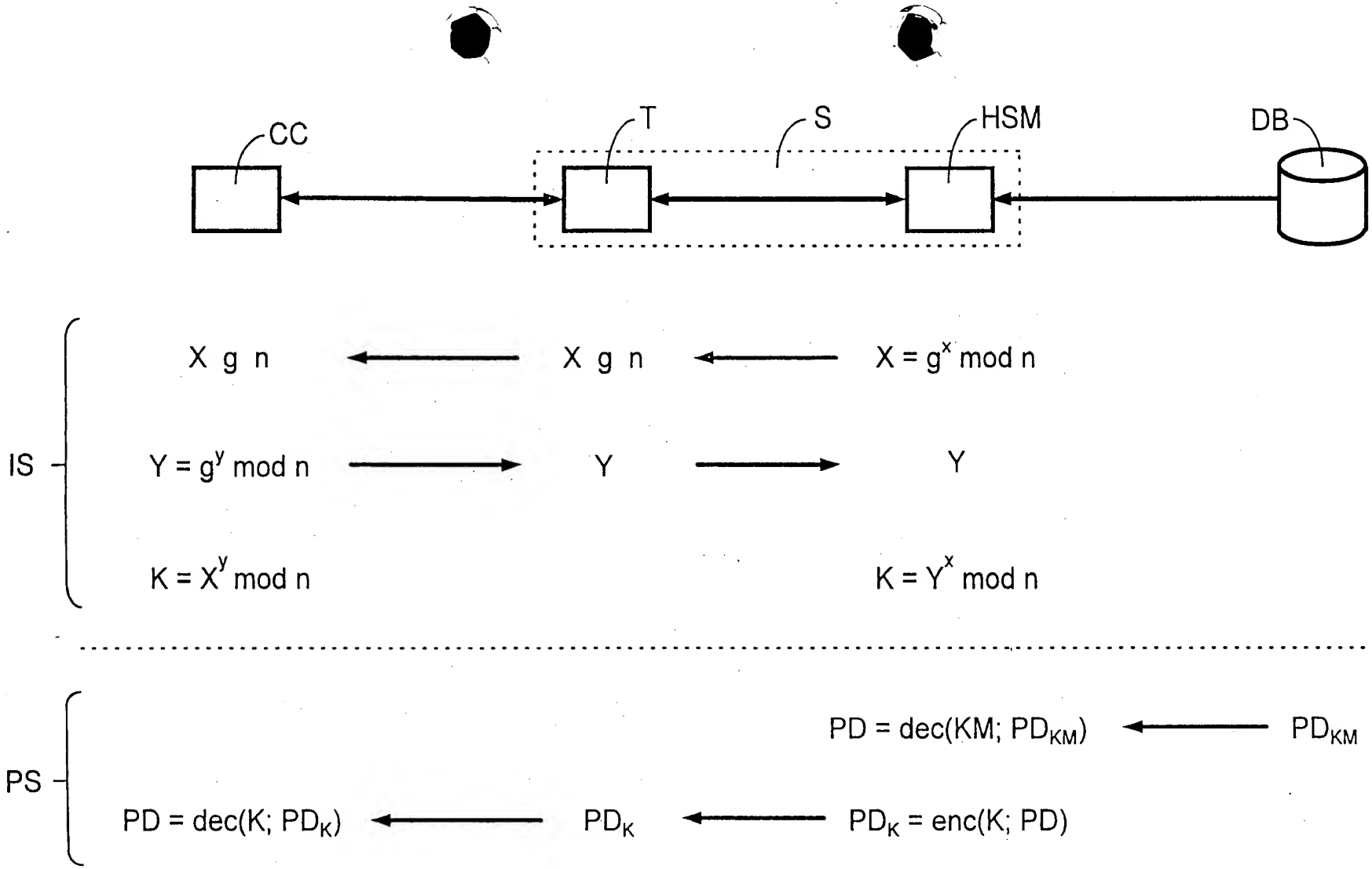
CC
T
S
HSM
DB
IS
X g n
X g n
X = g^x mod n
Y = g^y mod n
Y
Y
K = X^y mod n
K = Y^x mod n
PS
PD = dec(KM; PD_KM)
PD_KM
PD = dec(K; PD_K)
PD_K
PD_K = enc(K; PD)

Fig.